Federal Bureau of Investigation

Privacy Impact Assessment
for
JusticeConnect

Issued by:
Ernest J. Babcock, Privacy and Civil Liberties Officer

Approved by: Peter Winn, Acting Chief Privacy and Civil Liberties Officer, U.S. Department of Justice

Date approved: [January 26, 2018]

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The mission of the Online Services and Operations Unit (OSOU), Law Enforcement Support Section (LESS), Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) is to provide user-friendly means of electronic communication that offer a secure transmission of Sensitive But Unclassified information, to U.S. local, state, and federal law enforcement, criminal justice, and public safety communities throughout the world. OSOU develops and maintains systems that provide a vehicle for these communities to exchange information, conduct online education programs, and participate in professional special interest and topically focused dialog. In furtherance of its mission, OSOU is responsible for the implementation of JusticeConnect, an application which will allow authorized Law Enforcement Enterprise Portal (LEEP)[1] users to communicate and collaborate with each other in real time using components such as communities of interest, wikis, blogs, forums, and activities. The JusticeConnect application is accessible via LEEP.

This Privacy Impact Assessment (PIA) is being conducted to assess the privacy risks of JusticeConnect due to the nature of the information sharing that will occur within the application. JusticeConnect users provide their names, contact information, agency affiliation, and other personally identifiable information (PII). Additionally, users have the ability to share information for the administration of criminal justice functions and other official business purposes. The information that users share may contain PII about non-JusticeConnect users, such as missing persons, wanted persons, arrest reports, unknown individuals, agency contacts and organizational charts, and intelligence reports.

Section 1: Description of the Information System

The Purpose of JusticeConnect

JusticeConnect is an online user-driven, real time collaboration and communication tool. The purpose of JusticeConnect is to promote collaboration with and among the FBI's criminal justice, intelligence, national security, emergency management, military, public safety, and private sector partners by providing a real time environment in which to communicate with experts, create and join communities of common interest, create blogs to present ideas and receive feedback, share files with colleagues, and exchange ideas through online forums.

The JusticeConnect application allows users to communicate and collaborate with each other in real time using components such as communities of interest, wikis, blogs, forums, and activities. JusticeConnect provides users with ownership and control of the information they post. The application allows users to exchange ideas through online forums and communities of common interest;

[1] LEEP is a federated gateway that securely connects law enforcement, criminal justice, and homeland security communities to applications and services over the Internet. The benefits of LEEP include a single sign-on for users to access various services and systems, including JusticeConnect, and ensuring that only authenticated users have access to those systems and services. In order to participate in LEEP and to gain access to JusticeConnect, users must provide six identifying pieces of information: User ID, First Name, Last Name, User's Agency Email Address, User's Agency Telephone Number, and Employer/Agency Name.

communicate with experts; gather feedback from others through polls and surveys; create blogs to present ideas and receive feedback; share files with colleagues; and view, manage, organize and complete tasks quickly through activities applications.

Information Sharing within JusticeConnect

JusticeConnect consists of the following user-friendly components designed to facilitate collaboration and information sharing among its users: profiles, bookmarks, activities, wikis, files, communities, blogs, and forums.

Profiles: Each user in JusticeConnect will have a profile page that allows the user to share personally identifiable information about himself. A profile must include the user's name, phone number, email address, and agency affiliation, but can also include alternate telephone numbers and email addresses, address information, and additional professional information. Profile information also displays in other areas of JusticeConnect in which the user participates.

Bookmarks: The bookmark functionality allows users to save and share shortcuts to web content. Users can privately save bookmarks for their own personal use or they can make their bookmarks publicly available to other users. Users can search for publicly available bookmarks by keywords, tags,[2] and the name of the person who created the bookmark.

Activities: JusticeConnect allows users to form and share activity reminders. Activities act as a task management system which enables groups of people to easily collaborate on a task. Activities is a complete project management system. Users within an activity page can create entries, add content, assign to-do items, attach files, and share information such as websites and files. An activity page includes a list of all users involved in the activity.

Wikis: JusticeConnect provides users with the ability to create different internet pages about particular subjects. Wiki pages provide information on different topics. The creator of a Wiki controls who can modify the wiki page. For users with an owner or editor permission for a wiki page, users may add, edit, or comment on wiki pages. Teams can use wikis to create a central place to collaborate on a project.

Files: JusticeConnect includes a file-sharing service that permits users to upload, share, collaborate, tag, and comment on files. Users may upload files of nearly any type, including text, documents, data, presentations, PDFs, flash, graphics, audio, and video. To prevent malware intrusion JusticeConnect does not allow executable files or zip files to be uploaded. The file-sharing feature of JusticeConnect provides a means to share files, information, communications, and ideas with other members of a team without sending large files through e-mail. It also provides traceability of changes to a file, maintains

[2] Tags are keywords that a user places into a "tag" field when creating or sharing a bookmark, community, profile, activity, wiki, or other information within JusticeConnect. When a keyword in a tag field is searched, the tagged item will appear in the search results.

version control of files, and permits collaboration on files.[3]

Communities: Communities permit users to collaborate regarding a project or area of interest. A community may have its own media gallery, event calendar, blog, forums, bookmarks, activities, member list, wikis, and files. Three types of communities are available: public, moderated, and restricted. All users are able to view and join public communities. Information within moderated communities may be viewed by all users within the community, but users must be granted permission from the community owner to join the community. Restricted communities are not visible to anyone unless they are invited by the community owner to join the community.

Blogs: Blogs are online journals used to share information, generate ideas, or collect feedback on a topic. JusticeConnect supports blogging on a user's personal page or inside communities. A blog is a free text field.

Forums: Forums are provided within JusticeConnect to allow users to start discussions about a specific topic or to discuss areas of shared interest and concern. By participating in a forum, users can exchange ideas, ask questions, and leverage the expertise of other JusticeConnect users.

JusticeConnect also maintains audit logs of the system including login/logout attempts and all changes, additions, and deletions users make to information within JusticeConnect.

Access to JusticeConnect

JusticeConnect is available to authorized LEEP users. Authorized LEEP users of JusticeConnect are persons affiliated with the criminal justice system, intelligence professionals, military personnel, and governmental agencies associated with infrastructure protection of the United States. On a case by case basis, other individuals offering direct support to the criminal justice system may be given access to LEEP and JusticeConnect. The criminal justice system includes, but is not limited to, law enforcement agencies, including campus police departments, correctional agencies, probation and parole entities, and prosecuting attorney's offices on the federal, state, or local levels. Intelligence professionals from federal, state, tribal, or local governmental agencies are also eligible for access to LEEP and JusticeConnect. On a case by case basis, intelligence analysts working as contractors for federal, state, tribal, or local law enforcement or government agencies may be given access to LEEP and JusticeConnect. Active duty and civilian military personnel are eligible for access to LEEP and JusticeConnect. Soldiers in a reserve or National Guard status may be granted access to LEEP and JusticeConnect on a case by case basis. Emergency management personnel, including public safety directors and commissioners, and employees of state and local emergency management and first responder offices are eligible for access to LEEP and JusticeConnect. Select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety missions may be granted access to LEEP and JusticeConnect on a case by case basis.

---

[3] Uploaded files cannot be edited within JusticeConnect. To edit a file, the user must download the file, make changes, and upload the revised version to JusticeConnect. JusticeConnect logs all versions of files uploaded to the application. Users can see all previous versions of documents uploaded to JusticeConnect.

Authorized JusticeConnect users may include non-U.S. citizens employed by a U.S. criminal justice agency or approved federated Identity Provider (IdP).[4] All users accessing JusticeConnect through a federated IdP are fully vetted in accordance with CJIS Security Policy, including undergoing a fingerprint based background check.

All authorized LEEP users will have the option to opt into JusticeConnect through their LEEP profile pages. Individuals applying for a LeepID account via the LeepID IdP will also be able to select whether to join JusticeConnect on their LeepID application. Once an individual joins JusticeConnect, he will access JusticeConnect either via an icon in the services portlet[5] or from a tab in the navigational toolbar, both located on the LEEP homepage. JusticeConnect users have direct access to all public information within JusticeConnect. Information located in restricted communities within JusticeConnect will only be available to the members of the restricted community. System administrators will have access to all information within JusticeConnect and its audit logs.

Posting Information in and Retrieving Information from JusticeConnect

As stated above, the JusticeConnect application is accessible via LEEP. Once logged into JusticeConnect, users can post information and upload files within JusticeConnect. JusticeConnect provides users with ownership and control of the information they post while still maintaining the constraints of the *CJIS Security Policy,* the *LEEP Rules of Behavior,* and the *JusticeConnect Terms of Use*.

JusticeConnect includes a search bar that enables users to search for information via a key word search. Users can also search for other JusticeConnect users by name or other keyword. Information shared within JusticeConnect is only accessible through JusticeConnect, but users have the ability to print and save information from JusticeConnect. JusticeConnect also allows users to set email preferences to receive email notifications from JusticeConnect regarding updated content within the application.

Connections to other Systems

JusticeConnect is interfaced with LEEP and accessible as a service via LEEP. JusticeConnect does not connect to any other system, but it does utilize users' productivity suites and applications (such as e-mail and word processing). For example, if a user clicks on a document uploaded to JusticeConnect, the document will open with the applicable program on the user's operating system. If a user clicks on the email link within JusticeConnect, the user's email client on his operating system

---

[4] An IdP is defined as an organization/agency that creates, maintains, and vets information about each of its authorized users for LEEP access. Foreign user access to JusticeConnect is more strictly limited than LEEP access generally; specifically, it is limited to non-U.S. citizens vetted and employed by a U.S. criminal justice agency or approved U.S. agency identity provider. Sponsored foreign LEEP users accessing LEEP through the LeepID IdP, including foreign users residing outside of the U.S. and not employed by a U.S. criminal justice agency or approved identity provider, cannot access JusticeConnect.
[5] A portlet is a component of a portal web site that provides access to specific information sources or applications.

will open.

Type of System

JusticeConnect is defined as a major application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration	X	Financial account	X
Taxpayer ID	X	Driver's license	X	Financial transaction	X
Employee ID	X	Passport	X	Patient ID	X
File/case ID	X	Credit card	X		
Other identifying numbers (specify): None of the information above is required to be placed in JusticeConnect; however, the purpose of JusticeConnect is to provide real time collaboration among and between the FBI and its partners for official purposes. Therefore, it is possible that the above type of information may be shared within JusticeConnect to assist participating agencies in performing their official duties.					

General personal data					
Name	X	Date of birth	X	Religion	X
Maiden name	X	Place of birth	X	Financial info	X
Alias	X	Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service	X
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X	Education	X	Mother's maiden name	X
Other general personal data (specify): JusticeConnect only requires its users to provide their name, phone number, email address, and agency affiliation. All other information about users is voluntarily provided. The purpose of JusticeConnect is to provide real time collaboration among and between the FBI and its partners for official purposes. Therefore, it is possible that the above type of information on non-JusticeConnect users may be shared within JusticeConnect to assist agencies in performing their official duties.					

Work-related data					
Occupation	X	Telephone number	X	Salary	X
Job title	X	Email address	X	Work history	X
Work address	X	Business associates	X		
Other work-related data (specify): JusticeConnect only requires its users to provide their name,					

phone number, email address, and agency affiliation. All other information about users is voluntarily provided. The purpose of JusticeConnect is to provide real time collaboration among and between the FBI and its partners for official purposes. Therefore, it is possible that the above type of information on non-JusticeConnect users may be shared within JusticeConnect to assist agencies in performing their official duties.

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	X
Palm prints	X	Scars, marks, tattoos	X	Retina/iris scans	X
Voice recording/signatures	X	Vascular scan	X	Dental profile	X

Other distinguishing features/biometrics (specify): JusticeConnect only requires its users to provide their name, phone number, email address, and agency affiliation. All other information about users is voluntarily provided. The purpose of JusticeConnect is to provide real time collaboration among and between the FBI and its partners for official purposes. Therefore, it is possible that the above type of information on non-JusticeConnect users may be shared within JusticeConnect to assist agencies in performing their official duties. However, JusticeConnect only supports text based searches and retrieval of information. Information cannot be retrieved biometrically (e.g., by face recognition technology or the comparison of fingerprint images).

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	X

Other system/audit data (specify): This information will be maintained in system audit logs accessible only to specific administrative personnel.

Other information (specify)

Due to the nature of the input of information into the system, users are able to utilize free text fields to input any type of information they wish, as long as it falls within the boundaries of the Terms of Use, the CJIS Security Policy, and the Unclassified Information System policies. All information placed inside the system is only for criminal justice and other official business purposes of authorized users and is only shared among other users of JusticeConnect or as permitted by the system's routine uses as set forth in the FBI's Online Collaboration Systems System of Record Notice.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	X
Telephone		Email			
Other (specify): JusticeConnect is a web based interface that allows users to share information in an online environment. JusticeConnect users provide their own information, but information about non-JusticeConnect users is obtained from other investigative sources and data repositories.					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign			
Other (specify): Information within JusticeConnect is provided by JusticeConnect users who include authorized LEEP users as described in section 1 above. Authorized users may share information they receive from foreign government sources within JusticeConnect; however, foreign government sources do not directly provide information to JusticeConnect.					

Non-government sources					
Members of the public		Public media, internet		Private sector	X
Commercial data brokers					
Other (specify): As discussed above, authorized JusticeConnect users include select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety missions. These users will provide information within JusticeConnect. All authorized JusticeConnect users may share information they receive from members of the public, public media, and commercial data brokers within JusticeConnect; however, those non-government sources do not directly provide information to JusticeConnect.					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

JusticeConnect allows users to input information in free text fields as well as to upload files. The free text nature of JusticeConnect enables the potential for users to post sensitive, personally identifiable information (PII) about the user and about third parties. Users have the ability to post

significant PII in the wikis, files, communities, blogs, and forums, which poses a threat to privacy. However, JusticeConnect is to be used only for criminal justice and other official business purposes and information within JusticeConnect is only directly available to other JusticeConnect users. As discussed above, access to JusticeConnect is contingent upon LEEP membership and therefore restricted to individuals affiliated with the criminal justice system, intelligence professionals, military personnel, governmental agencies associated with infrastructure protection of the United States, other individuals offering direct support to the criminal justice system, and select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety missions. Due to the purpose of the system, the amount and type of information users will share will vary widely. In order to mitigate the risks of over collection of PII and limit access to PII, all users must agree to the JusticeConnect Terms of Use. The Terms of Use require that users post only the minimum amount of sensitive information or PII required to further the official purpose for which the information is being shared. The Terms of Use also require users to review documents before sharing them within JusticeConnect and to redact any sensitive information or PII not necessary to achieve the official purpose for which the information is being shared. Additionally, the Terms of Use limit the use of information from JusticeConnect to the administration of criminal justice functions and other official business purposes of authorized JusticeConnect users. All users accessing LEEP are vetted by their identity provider to ensure that they meet the eligibility requirements for a LEEP membership. All LEEP users are required to agree to the LEEP Rules of Behavior before they first access LEEP and once per year thereafter. For user reference, a link to the JusticeConnect Terms of Use and Privacy Statement is available at the bottom of every page on JusticeConnect.

JusticeConnect is an unclassified system, but JusticeConnect users may include authorized LEEP users who have access to classified information. Consequently, there is a risk that classified information could be posted within JusticeConnect. To remind users that only unclassified information can be shared within JusticeConnect and to provide a mechanism by which users can report classified information found on JusticeConnect, JusticeConnect displays a banner at the top of every page that says, "JusticeConnect is an UNCLASSIFIED system. Any classified information that is found within should be reported immediately [by phone or email]." In order to mitigate the risk of classified information being loaded into a file and shared within JusticeConnect, a security feature automatically scans uploading files for words that have been specified in a pre-determined list. If one of the words on that list is found within the file, the file is removed from the software within seconds of it being posted. Generally, the scan is completed before the document is viewable by the JusticeConnect community. If a user posts one of the words found on the list into a free text field, a notice is automatically sent to a specified oversight group containing the location of the information as well as the user information. The information is then reviewed by the JusticeConnect Content Monitoring Team and the spillage portion of the Incident Response Plan is followed.

JusticeConnect users will also be able to report information that violates the JusticeConnect Terms of Use. Within communities users have the ability to flag community content as inappropriate. The Content Monitoring Team reviews the flagged information and removes any content that violates the Terms of Use. If users see information outside of communities that they think is inappropriate, they will contact the FBI Support Center via email or phone and the system Incident Response Plan will be implemented. A notice is sent to a specified oversight group containing specific information about the content as well as the user information. JusticeConnect's designated Content Monitoring Team reviews the content and removes any information that violates the JusticeConnect Terms of Use. The FBI Content Monitoring Team also routinely monitors the content posted within JusticeConnect for any

information that is classified higher than Unclassified/FOUO classification and/or violates the JusticeConnect Terms of Use. If the FBI Content Monitoring Team identifies any information that violates the system's classification level or Terms of Use, the team will follow the Content Monitoring Standard Operating Procedure. System administrators have access to all user activity through the Actiance Vantage software. User activity audit logs are monitored and accessible only to the JusticeConnect operational team.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	[ ]	For civil enforcement activities
X	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
[ ]	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	X	For administering human resources programs
[ ]	For litigation		
[ ]	Other (specify): [ ]		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

JusticeConnect provides authorized LEEP users with a user-driven, real time collaboration and communication tool. Currently, there are no services or resources available on LEEP that allow for such activities. Expanding available collaboration tools between the FBI and its partners enables the FBI to carry out its national security and criminal justice missions. JusticeConnect allows the FBI and its partners to communicate with experts, create and join communities of common interest, create blogs to present ideas and receive feedback, share files with colleagues, and exchange ideas through online forums. By providing a restricted online environment in which to share information for criminal justice and other official business purposes, JusticeConnect increases efficiency in communication and collaboration among the FBI and its partners.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
x	Statute	42 U.S.C. § 3771; 28 U.S.C. § 534; 44 U.S.C. § 3301; 5 U.S.C. § 301; Federal Information Security Modernization Act of 2014
	Executive Order	
x	Federal Regulation	28 C.F.R. § 0.85; 28 C.F.R., Part 20
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Information within JusticeConnect will be retained for 25 years in accordance with the applicable retention schedules approved by the National Archives and Records Administration (NARA). JusticeConnect users may remove information they have shared from the graphical user interface (GUI) within JusticeConnect; however, the shared information will be retained in the JusticeConnect audit logs for 25 years. JusticeConnect users who subsequently opt out of JusticeConnect will not be searchable within the GUI; however, information they previously posted within JusticeConnect remains viewable within the GUI. Information that the FBI Content Monitoring Team removes from JusticeConnect for violation of the Terms of Use will not be available in the GUI; however, it will remain in the JusticeConnect audit logs for 25 years. Any information removed from JusticeConnect because it is classified is also removed from all audit logs.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's National Institute of Standards and Technology (NIST) 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

JusticeConnect allows users to input information in free text fields, as well as to upload files. The free text nature of JusticeConnect enables the potential for users to post sensitive, personally identifiable information (PII) about the user and about third parties. It is anticipated that users may post significant PII in the wikis, files, communities, blogs, and forums. However, JusticeConnect is to be used only for criminal justice and other official business purposes and information within JusticeConnect is only directly available to other JusticeConnect users. The Terms of Use limit the use of information from JusticeConnect to the administration of criminal justice functions and other official business purposes of authorized JusticeConnect users. As discussed above, access to JusticeConnect is contingent upon LEEP membership and therefore restricted to individuals affiliated with the criminal justice system, intelligence professionals, military personnel, governmental agencies associated with infrastructure protection of the United States, other individuals offering direct support to the criminal justice system, and select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety missions. All JusticeConnect users access JusticeConnect through an authorized LEEP IdP. An IdP is defined as an organization/agency that creates, maintains, and vets information about each of its authorized users for LEEP access. The IdP also assigns the current attributes about the individual for a given information technology session. These attributes are presented when the user accesses LEEP via a secure web browser session at a designated URL, which then allows them access to JusticeConnect. LEEP performs user authentication each time an individual logs into LEEP. LEEP usage is monitored and audit logs are scanned to detect unusual activity. Alerts identifying unusual activity are sent to system security personnel and system administrators.

JusticeConnect users are required to agree to the LEEP Rules of Behavior once per year, and to acknowledge and follow the JusticeConnect Terms of Use, which restrict the sharing of PII to information that is necessary to achieve the official purpose for which it is shared. All users must agree to the LEEP Rules of Behavior before accessing LEEP and agree to the JusticeConnect Terms of Use and a government system notice prior to being allowed access to JusticeConnect. For user reference, a link to the Terms of Use and Privacy Statement is available at the bottom of every page. All users must abide by the LEEP Rules of Behavior and the JusticeConnect Terms of Use. Privileged users are required to take annual training on contingency planning, incident response, data spill management, and information security. General FBI users are required to take information security training annually. Non-FBI users are required to abide by the training requirements set forth in the CJIS Security Policy.

JusticeConnect permits users to upload files. Consequently, there is a risk that PII within JusticeConnect may be compromised by the introduction of malicious software into the system through an uploaded file. To mitigate this risk, an Enterprise and server-based Anti-Virus (AV) and Malware detection solution is leveraged. This AV and Malware solution scans all files being uploaded into the JusticeConnect environment for malicious software in real time. Any files that contain malicious software are prevented from being uploaded to JusticeConnect.

PII Confidentiality Risk Level: ☐ **Low** ☑ **Moderate** ☐ **High**

Access controls

x	Access Enforcement: The system employs Privileged User role-based access controls (RBAC) for System Administrators and Database Administrators (DBA). Privileged users have no ability to access the underlying database from the front-end interface. The back-end interface is Secure Shell (SSH) constrained using unique identifiers and authenticators. For general users (GENUSERs), access control is inherited from LEEP, which permits the Federated LEEP Users access to the JusticeConnect environment.
x	Separation of Duties: JusticeConnect, by its Social Media nature, creates a risk that users will post significant PII as described in sections 2.3 and 3.5 of this document. Due to the purpose of the system, it will be difficult to limit the amount and type of information users will share. In order to mitigate the threats to privacy, access to JusticeConnect is only available to authorized LEEP users. Privileged user access to the underlying database is role based and controlled by access control lists.
x	Least Privilege: User roles enforce the most restrictive set of rights/controls for each user group. General User access is inherited from LEEP- JusticeConnect is accessible through LEEP. Privileged User access is limited to a limited group of Database Administrators and System Administrators. The JusticeConnect Content Monitoring Team is comprised of database and system administrators.
x	Remote Access: Remote access to JusticeConnect is inherited from LEEP. JusticeConnect inherits data encryption via 443 (HTTPS) from LEEP. LEEP enforces Transport Layer Security (TLS) 1.2 for access on the External Webseals. JusticeConnect is a Law Enforcement/FBI social media service that resides behind LEEP's Identity and Access Management (IAM) function. Remote Access is only permitted as a GENUSER and is secured by LEEP two factor authentication (2FA) using a one-time password (OTP) or electronic authentication assurance level code (EAUTH) Level 3 attribute via single sign-on (SSO). All privileged user functions are restricted to SSH and are not permitted via the Web user interface.
x	User-Based Collaboration and Information Sharing: Automated mechanisms, which utilize metadata and Security Assertion Markup Language (SAML), are in place for matching access authorizations to contractual/MOU/MOA restrictions. Inherited from LEEP, this is accomplished via LEEP Federated SSO access via IdP agreements established via CJIS Security Policy for State, Local, Tribal, and Municipal agencies and set forth in MOU/MOA with participating United States Government agencies subject to NIST and the Federal Information Security Modernization Act (FISMA). The global federated identity and privilege management (GFIPM) attributes exist within the IdP SAML that permits access to selected services residing within LEEP.
x	Access Control for Mobile Devices: Access to JusticeConnect is derived via 2FA authenticated LEEP sessions. The nature of LEEP is to provide authorized and authenticated remote mobile device access to services via multiple types of mobile devices.

Audit controls

x	Auditable Events: Operating System and Database auditing is compliant with standards set by the FBI Records Management Division, NARA, and CJIS Enterprise Audit Unit. Audit logs are maintained for 25 years. Committee on National Security Systems Instruction (CNSSI) Auditable events are sent to Enterprise Logging. Oracle DB and IBM DB2 logs are maintained in human readable format (XML) and stored within ESAN. Additional controls listed in section 2.3 trigger auditable events.
x	Audit Review, Analysis, and Reporting: Audit records are regularly reviewed for inappropriate or unusual activity affecting PII; such activity is investigated and reported and responsive action and appropriate mitigation is taken. Log monitoring occurs daily during the week. Events are monitored 24/7 by the system security administrators and the operations and maintenance team.

Identification and Authentication controls

x	Identification and Authentication: Users are uniquely identified before accessing JusticeConnect; remote access requires 2FA and 30-minute "time-out" functionality. Inherited from LEEP, access to JusticeConnect is derived via 2FA authenticated LEEP sessions. GENUSER sessions rely on federated identity management/SSO access from LEEP. JusticeConnect does not itself enforce GENUSER access using an identity management application or authentication module; however, it is only accessible by authorized LEEP Federation Users. For LEEP Federated (SSO) users, authenticators are managed as directed by CJIS Security Policy. For Federated IdP users accessing LEEP via cjis.gov, LEEP enforces authenticator management at the enterprise application interface (EAI). Privileged user accounts are managed by the system security administrator.
Other: JusticeConnect session termination is dependent on LEEP access and LEEP session termination for automatic session termination. Once access to JusticeConnect has begun, the session remains active during an active LEEP session. If a user is idle in JusticeConnect for 30 minutes, the session does not terminate as long as a user is active elsewhere in LEEP. JusticeConnect provides a user initiated logout that terminates the session and dumps session information. Once logged out, users are required to return to LEEP to gain access to JusticeConnect. The application does employ a User initiated Session Termination function (Logout). JusticeConnect access is strictly a session based assertion and information is not stored in a persistent cookie.	

Media controls

x	Media Access: Access to system media (CDs, USB flash drives, backup tapes) is restricted. JusticeConnect backup instances are Enterprise Storage Services (ESS) controlled.
x	Media Marking: Media containing PII is labeled.
x	Media Storage: Media containing PII is securely stored.
x	Media Transport: Media is encrypted and stored in a locked container during transport.
x	Media Sanitation: Media is sanitized prior to re-use

Data Confidentiality controls

x	Transmission Confidentiality: JusticeConnect inherits data encryption via 443 (HTTPS) from LEEP. LEEP enforces TLS 1.2 for access on the External Webseals. From UNET and CJIS UNet (Internal Webseals) SSL/TLS is enforced for access.
x	Protection of Information at Rest: Access to JusticeConnect's front-end interface is controlled by user authentication. JusticeConnect backup instances are ESS controlled. Physical disk drives are protected by physical security measures.

Information System Monitoring

x	Information System Monitoring: Inherited from LEEP/Shared Enterprise Network (SEN), the security architecture represents a Defense-in-Depth information technology security philosophy. JusticeConnect resides within the SEN and LEEP security boundaries but is virtually separated from other applications. JusticeConnect is supported by the SEN and LEEP environments and assumes a defense in depth architecture enforced at the SEN Level. SEN is supported through industry standard IS network layout for Public facing and Internal User access. Monitoring for all elements on JusticeConnect is enforced within SEN.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	[X]	[ ]	[X]	JusticeConnect users have direct access to JusticeConnect and any information publicly available within JusticeConnect. Some features of JusticeConnect allow users to restrict information to certain users within JusticeConnect. JusticeConnect users may copy, print, or download information from JusticeConnect. Copied, printed or downloaded information may be shared with non-JusticeConnect users for criminal justice or other official business purposes.
DOJ components	[X]	[ ]	[X]	JusticeConnect users from DOJ components have direct access to information within JusticeConnect. Some features of JusticeConnect allow users to restrict information to certain users within JusticeConnect. JusticeConnect

				users may copy, print, or download information from JusticeConnect. Copied, printed or downloaded information may be shared with non-JusticeConnect users for criminal justice or other official business purposes.
Federal entities	[X]	[ ]	[X]	JusticeConnect users from federal entities have direct access to information within JusticeConnect. Some features of JusticeConnect allow users to restrict information to certain users within JusticeConnect. JusticeConnect users may copy, print, or download information from JusticeConnect. Copied, printed or downloaded information may be shared with non-JusticeConnect users for criminal justice or other official business purposes.
State, local, tribal gov't entities	[X]	[ ]	[X]	JusticeConnect users from state, local, and tribal gov't entities have direct access to information within JusticeConnect. Some features of JusticeConnect allow users to restrict information to certain users within JusticeConnect. JusticeConnect users may copy, print, or download information from JusticeConnect. Copied, printed or downloaded information may be shared with non-JusticeConnect users for criminal justice or other official business purposes.
Public	[ ]	[ ]	[ ]	[ ]
Private sector	[X]	[ ]	[X]	As discussed above, JusticeConnect users include select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety missions. JusticeConnect users may copy, print, or download information from JusticeConnect. Copied,

				printed or downloaded information may be shared with non-JusticeConnect users for criminal justice or other official business purposes.
Foreign governments	[ ]	[ ]	[ ]	[ ]
Foreign entities	[ ]	[ ]	[ ]	[ ]
Other (specify):	[X]	[ ]	[ ]	On a case-by-case basis, JusticeConnect users may copy, print, or download information from JusticeConnect. Copied, printed or downloaded information may be shared with non-JusticeConnect users for criminal justice or other official business purposes.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

JusticeConnect is interfaced with LEEP and is only accessible as a service via LEEP. Access to LEEP is gained through an IdP and requires the use of multi-factor authentication for access. The IdP performs user authentication each time an individual logs into LEEP. User attributes are presented when the user accesses LEEP via a secure web browser session at a designated URL, subsequently permitting access to JusticeConnect if the LEEP user has opted in to JusticeConnect.

As discussed above, access to JusticeConnect is contingent upon LEEP membership and therefore restricted to individuals affiliated with the criminal justice system, intelligence professionals, military personnel, governmental agencies associated with infrastructure protection of the United States, other individuals offering direct support to the criminal justice system, and select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety missions. All users accessing LEEP are vetted by their identity provider to ensure that they meet the eligibility requirements for a LEEP membership. All users must agree to the JusticeConnect Terms of Use which restrict the sharing of PII to information that is necessary to achieve the official purpose for which it is shared. Additionally, all LEEP users are required to agree to the LEEP Rules of Behavior before they first access LEEP and once per year thereafter. For user

reference, a link to the JusticeConnect Terms of Use and Privacy Statement is available at the bottom of every page on JusticeConnect.

The information inside JusticeConnect is only directly available to authorized users. The Terms of Use limit the use of information from JusticeConnect to the administration of criminal justice functions and other official business purposes of authorized JusticeConnect users. This may include sharing information from JusticeConnect with non-JusticeConnect users if the non-JusticeConnect users have a need to know the information in furtherance of a JusticeConnect user's criminal justice or official business purpose. Users cannot share information with non-JusticeConnect users directly from JusticeConnect. However, JusticeConnect users can download, copy, and print information from JusticeConnect, which may then be shared with non-JusticeConnect users with a need to know the information. JusticeConnect also sends emails to users based on subscriptions they set. Users could forward the email to non-JusticeConnect users; however, links to items within JusticeConnect will not work unless an individual logs into JusticeConnect.

In addition to signing the LEEP Rules of Behavior once per year, JusticeConnect users are required to agree to the Terms of Use and acknowledge a System Use Notification prior to being allowed access to JusticeConnect. A banner has been placed at the top of every page inside JusticeConnect reminding users that the system is for Unclassified information only.

System records are maintained in limited access space in FBI controlled facilities and offices. Computerized data is password protected and requires two-factor authentication for access. Remote access through the Internet is provided via the encrypted communications protocol Hypertext Transfer Protocol with Transport Layer Security (HTTPS). All FBI personnel are required to pass an extensive background investigation. The information is accessed only by authorized DOJ personnel or by non-DOJ personnel properly authorized to access the system. System audit logs are created and monitored to detect any misuse of the system.

JusticeConnect leverages an Enterprise and server-based AV and Malware detection solution. This Enterprise AV and Malware solution scans all files being uploaded into the JusticeConnect environment for malicious software in real time. Any files that contain malicious software are prevented from being uploaded to JusticeConnect.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.

X	Yes, notice is provided by other means.	Specify how: JusticeConnect users are provided with a Privacy Act statement upon their initial connection to JusticeConnect. A Privacy Statement link is also available at the bottom of every webpage within JusticeConnect. Additionally, all users agree to a government system notice that they have no reasonable expectation of privacy for information shared within JusticeConnect and that their use of JusticeConnect data shared within JusticeConnect may be monitored, intercepted, searched, and/or seized. Non-JusticeConnect users whose information appears in JusticeConnect are provided notice that their information may appear in JusticeConnect through the System of Records Notice and this Privacy Impact Assessment.
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: JusticeConnect users must opt in to participate in JusticeConnect. If a LEEP user does not decide to join JusticeConnect, his/her information will not appear in JusticeConnect. All information provided by JusticeConnect users other than name, phone number, email address, and agency affiliation, is voluntarily provided. JusticeConnect users may cease participation in JusticeConnect at any time by opting out of JusticeConnect on their LEEP profile page.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Non-JusticeConnect users will not have the opportunity to decline to provide information. The information is collected and shared for criminal justice, national security, and other official business purposes in accordance with federal and state laws and the JusticeConnect Terms of Use.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

[X]	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: Users have the ability to control the settings of files they share in order to allow or disallow other users to share the information. In addition, users can restrict the information they share by placing it in a restricted community and only allowing a specific audience access to the information. All information within JusticeConnect is voluntarily shared by JusticeConnect users.
[X]	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Non-JusticeConnect users will not have the opportunity to consent to particular uses of their information. The information is collected, shared and utilized for criminal justice and other official purposes in accordance with federal and state laws and the JusticeConnect Terms of Use.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

All JusticeConnect users voluntarily join JusticeConnect and provide their information. The first time a user logs into LEEP, the user must agree to the LEEP Rules of Behavior. The first time a user logs into JusticeConnect, the user must agree to the JusticeConnect Terms of Use. The JusticeConnect Terms of Use include a Privacy Act statement informing users that information posted within JusticeConnect will be shared with other JusticeConnect users and disclosed in accordance with routine uses published in the Federal Register. Users also acknowledge a government system notice informing them that they have no reasonable expectation of privacy for information shared within JusticeConnect and that their use of JusticeConnect data shared within JusticeConnect may be monitored, intercepted, searched, and/or seized. Any user who decides that he does not wish to continue to share information in JusticeConnect may opt out of participation at any time.

Information in JusticeConnect may include PII on non-JusticeConnect users who do not have access to the system and therefore do not have an ability to control the use of their information within

JusticeConnect or consent to the use of their information. The System of Records Notice covering JusticeConnect, the Notice of Proposed Rule Making to exempt this system from certain provisions of the Privacy Act under limited circumstances, and this Privacy Impact Assessment provide notice to non-JusticeConnect users that some information about them may be shared within JusticeConnect. PII on non-JusticeConnect users is only allowed to be shared for criminal justice and other official business purposes. JusticeConnect users are required to limit the sharing of third party PII to information necessary to achieve the official purpose for which the information is being shared. The JusticeConnect Terms of Use direct users to review all files prior to uploading and to redact any PII that is not necessary to the purpose for which the file is being shared. Because JusticeConnect supports criminal justice, law enforcement, and national security purposes, it is not feasible to inform non-JusticeConnect users of the use of their PII within JusticeConnect.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted. JusticeConnect underwent a formal authority to operate (ATO) Security Assessment and Authorization (SAA). This assessment requires that all applicable controls outlined within the tailored system requirement specification (SRS) based on the Federal Information Processing Standards (FIPS) 199 Categorization are addressed to ensure operational compliance within applicable NIST 800-53 REV4 Security Controls.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: JusticeConnect underwent a formal ATO Security Assessment and Authorization (SAA). This assessment requires that all applicable controls outlined within the tailored SRS based on the FIPS 199 Categorization are addressed to ensure operational compliance within applicable NIST 800-53 REV4 Security Controls.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: JusticeConnect underwent a formal ATO Security Assessment and Authorization (SAA). This assessment requires that all applicable controls outlined within the tailored SRS based on the FIPS 199 Categorization are addressed to ensure operational compliance within applicable NIST 800-53 REV4 Security Controls.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: JusticeConnect underwent a formal ATO Security Assessment and Authorization (SAA). A three year ATO authorizing operational state was awarded on March 15, 2017.
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Adheres to CJIS policy on audit and local backup to Enterprise Storage Services/Enterprise Backup Services (ESS/EBS) and additionally employs Splunk, Nagios, and Tripwire to provide monitoring, reports, and alerts on Role-based and Privileged User level access as needed, changes to file integrity, and system security performance.

X			Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.
X			Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.
X			The following training is required for authorized users to access or receive information in the system:
	X		General information security training
	X		Training specific to the system for authorized users within the Department.
	X		Training specific to the system for authorized users outside of the component.
	X		Other (specify): Annual Privileged User Training/Annual InfoSec Training: Privileged Users are system specific and limited to System Administrators and Database Administrators, the JusticeConnect Content Monitoring Team, and the JusticeConnect operations and maintenance team. Privileged users require initial training and annual review training. Information Security (InfoSec) Awareness training is applicable to all users of U.S. Government Information Systems.

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

JusticeConnect, as a U.S. Government Information System, adheres to FBI Security Assessment and Authorization and is subject to the 2002 Federal Information Security Management Act (FISMA), as amended in 2014, to secure the Information System from unauthorized access and meet technical, management, and operational compliance with NIST SP 800-53 Security Controls. Specifically, the Security Assessment and Authorization process applicable to LEEP—and, thus, JusticeConnect—provides for continuous monitoring, evaluation and review of the implemented security controls for the identified information systems. It also provides for the evaluation and implementation of technical and non-technical security features and safeguards that are used to meet the specified set of security requirements. The Security Assessment and Authorization process is integrated into the life-cycle of this information system. The process serves as quality control for system security, ensuring the identification and integration of security related features and procedures that are to be implemented to provide the needed level of security.

Access Control enforcement is also inherited from LEEP. LEEP access controls include two-factor authentication, role based access controls for privileged users, and other controls as discussed in section 3.5 above.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

[X] Yes, and this system is covered by an existing system of records notice.

Provide the system name and number, as well as the Federal Register citation(s) for the most recent

complete notice and any subsequent notices reflecting amendment to the system:

JUSTICE/FBI-004, *FBI Online Collaboration Systems*, 82 Fed. Reg. 57291 (Dec. 4, 2017).

Yes, and a system of records notice is in development.

☐ No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information within JusticeConnect is retrieved by search functionality. The search functionality within the application allows users to search for other users or information shared within JusticeConnect by name, other personal identifiers, keyword, or tag.